

REMARKS

Claims 1-7, 10-19, 22-31, 34-36, and 40-44 are pending. Claims 8, 9, 20, 21, 32, 33, and 37-39 were previously cancelled without prejudice. Claims 1, 13, 25, and 40 are independent claims. Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1, 2, 13, 14, 25, and 26 stand rejected under 35 USC 102(e) as allegedly being anticipated by Peyravian et al. (US 2004/0158715), hereinafter "Peyravian." Claims 6, 7, 10, 18, 19, 22, 30, 31, 34, and 40 stand rejected under 35 USC 103(a) as allegedly being unpatentable over Peyravian. Claims 3-5, 11, 12, 15-17, 23, 24, 27-29, 35, and 36 stand rejected under 35 USC 103(a) as allegedly being unpatentable over Peyravian in view of Schneier, ("Applied Cryptography," 2nd edition, pages 38-41 and 146), hereinafter "Schneier." Claims 41-44 stand rejected under 35 USC 103(a) as allegedly being unpatentable over Peyravian in view of Palekar (US 2003/0226017), hereinafter "Palekar." The rejections are respectfully traversed. Peyravian, Schneir, or Palekar, taken alone or in any combination, do not describe or suggest all the features of the claimed subject matter.

Claim 1 recites "establishing a tunnel between an authenticator in the network and a device, the tunnel using a tunnel protocol, the authenticator having a first public key, the device having a second secret and a second public key; generating a first hash for transmission to the device, the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol; comparing the first hash with a second hash, wherein the second hash is generated at the device; and upon determining that the first hash matches the second hash, establishing an authenticated session between the

device and the authenticator." (Emphasis added). Peyravian describes a method to exchange and authenticate public cryptographic keys between parties that share a common but secret password. See, Peyravian at Abstract. Peyravian does not describe all the features of claim 1.

The Office Action states:

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the server does not obtain the password from a user to generate a first hash) are not recited in the rejected claim(s).

See, Office Action, page 2, "Response to Arguments."

Thus, the Office Action contends that features that are not recited in the claims are relied upon to overcome the rejections. This contention should be reconsidered. Claim 1 recites, in part, "generating a first hash for transmission to the device, the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol." In contrast, Peyravian does not describe obtaining the password from a user because, in Peyravian, the server and the user know the common password a priori. It is respectfully submitted that "the first hash generated using a secret obtained from a user" is, in fact, recited in the rejected claims, and that Peyravian does not describe this feature.

Further, it is respectfully submitted that the Office Action has not addressed all the features of the claimed subject matter. In this regard, the Office Action states:

The client concatenates the public key of the client, the public key of the server, and a random number ([0038] & [0040]), which is then hashed by the client and transmitted to the server ([0040]), ... (Emphasis added).

See, Office Action, page 3, first paragraph.

Thus, the Office Action contends that Peyravian describes a random number. However, the claimed subject matter recites, in part, "a random number generated from the tunnel protocol." Since the Office Action does not address this feature of claim 1, the Office Action does not provide sufficient reasons for rejecting claim 1 in compliance with 35 USC 132. Therefore, the rejection is improper. Further, it is respectfully submitted that the cited portions of Peyravian (see, Peyravian, [0038], [0040]) do not describe that the random number is generated from the tunnel protocol. In contrast, Peyravian describes a random number, Rc, generated by the client or on behalf of the client and a random number, Rs, generated by the server or on behalf of the server. Peyravian does not describe that either Rc or Rs are generated from the tunnel protocol.

Furthermore, the Office Action contends that Peyravian teaches "the authenticator having a first public key, the device having a second secret and a second public key," as claimed because Peyravian teaches that the client and the server each have a public/private key pair and a shared secret. See, e.g., Office Action, page 2, last paragraph - page 3, first paragraph. This contention should be reconsidered. The cited portions of Peyravian teach "PW-secret one-time-use password that is known by both the client and the server," "PKc-initial public key component of the client's public/private key pair," and "PKs-initial public key component of the server's public/private key pair." See, Peyravian, [0022], [0023], and [0025], respectively. In Peyravian, the secret, PW, is not obtained from a user because Peyravian describes that the server and the client already possess the secret. In contrast, as claimed, a secret is obtained from a user to generate a first hash. Thus,

"secret, PW," as taught by Peyravian is not equivalent to "the second secret," as claimed.

Peyravian states "...a client and a server know a common password a priori." See, Peyravian, [0011]. (Emphasis added). Thus, in Peyravian, the common password is already known to both the client and the server before establishing any connection between the client and the server. Further, Peyravian states "A secret password, which may be distributed over a secure channel, is assumed to be known by both the client and the server." See, Peyravian, [0016]. Thus, in Peyravian, the server does not obtain the password from a user to generate a first hash because both, the server and the client, already possess the secret. In contrast, as claimed, a secret is obtained from a user for generating a first hash.

In addition, Peyravian states:

As shown in FIG. 1, a password PW, which may be random, is generated using current practices (step 100), and distributed securely to the client and to the server (step 105). For example, the server may generate and send the pair (ID, PW) to the client using conventional mail, email, or telephone.

See, Peyravian, [0033].

Thus, as described in Peyravian, the password is generated and distributed to both the server and the client. In fact, Peyravian describes an example where the server sends the pair (ID, PW) to the client.

Thus, Peyravian does not describe or suggest "the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol," as claimed. Since the server is already in possession of the password, the server certainly does not receive the password from the client.

Thus, Peyravian does not describe all the features of claim 1. Therefore, anticipation is not established. Accordingly, claim 1 should be allowable. Claims 2-7 and 10-12 should also be patentable at least for similar reasons and for the additional recitations that they contain.

Claim 3 depends from claim 1. Peyravian does not describe or suggest all the features of claim 3 for reasons similar to claim 1. Schneier does not rectify the deficiencies in Peyravian. In this regard, the cited portions of Schneier do not describe or suggest "the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol," as claimed. Therefore, the suggested combination of Peyravian and Schneier does not describe or suggest all the features of claim 3. Accordingly, claim 3 should also be patentable.

Claim 13 recites "establish a tunnel between an authenticator in the network and a device, the tunnel using a tunnel protocol, the authenticator having a first public key, the device having a second secret and a second public key; generate a first hash for transmission to the device, the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol; compare the first hash with a second hash, wherein the second hash is generated at the device; and upon determining that the first hash matches the second hash, establish an authenticated session between the device and the authenticator." (Emphasis added).

Claim 13 should be patentable at least for reasons similar to claim 1. Claims 14-19, 23, and 24 should also be patentable at least for similar reasons and for the additional recitations that they contain.

Claim 25 recites "establish a tunnel between an authenticator in the network and a device, the tunnel using a tunnel protocol, the authenticator having a first public key, the device having a second secret and a second public key; generate a first hash for transmission to the device, the first hash generated using the a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol; compare the first hash with a second hash, wherein the second hash is generated at the device; and upon determining that the first hash matches the second hash, establish an authenticated session between the device and the authenticator." (Emphasis added).

Claim 25 should be patentable at least for reasons similar to claim 1. Claims 26-31 and 34-36 should also be patentable at least for similar reasons and for the additional recitations that they contain.

Claim 40 recites "a display; memory; a processor configured to connect the product to a secure network by performing operations comprising: establishing a tunnel between an authenticator in the network and the product, the tunnel using a tunnel protocol, the authenticator having a first public key, the product having a second secret and a second public key; generating a first hash, the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol to produce a hash of the first secret; comparing the first hash with a second hash, wherein the second hash is generated at the product; and upon determining that the first hash matches the second hash, establishing an authenticated session between the product and the authenticator." (Emphasis added).

Claim 40 should be patentable at least for reasons similar to claim 1 and for the additional recitations that it contains. Claims 41-44 should also be patentable at least for similar reasons and for the additional recitations that they contain.

For example, claim 41 depends from claim 40 and should be patentable for reasons similar to claim 40. Peyravian does not describe or suggest all the features of claim 40 for reasons similar to claim 1. Palekar does not rectify the deficiencies in Peyravian.

Palekar describes that an authentication protocol can be used to establish a secure method of communication between two devices on a network. Once established, the secure communication can be used to authenticate a client through various authentication methods. See, e.g., Palekar at Abstract. Palekar does not describe or suggest "the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol to produce a hash of the first secret," as claimed. Therefore, the suggested combination of Peyravian and Palekar does not describe or suggest all the features of the claimed subject matter. Accordingly, claim 41 should also be patentable. Claims 42-44 should also be patentable at least for similar reasons.

CONCLUSION

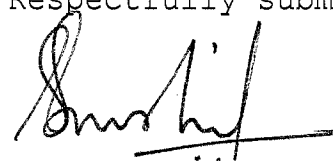
It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, Applicants respectfully submit that the application is in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Please apply any credits or additional charges to deposit account 06-1050.

Respectfully submitted,

Date: Nov. 30 '07.



Sushil Shrinivasan
Reg. No. L0368

Fish & Richardson P.C.
PTO Customer No.: 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile